Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
In the Matter of Petition for Expedited	)	
Rulemaking to Establish Technical	)	RM-11376
Requirements and Standards Pursuant to	)	
Section 107(b) of the Communications	)	
Assistance for Law Enforcement Act	)	

To: The Commission

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Of Counsel:
Thomas M. Barba
Chung Hsiang Mah
Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036
Tel: 202-429-3000
Fax: 202-429-3902

Grant Seiffert, President
Danielle Jafari, Senior Director
and General Counsel, Government Affairs
Telecommunications Industry Association
2500 Wilson Blvd., Suite 300
Arlington, VA 22201
Tel: 703-907-7700
Fax: 703-907-7727

July 20, 2007

TABLE OF CONTENTS

SUMMARY

The Telecommunications Industry Association ("TIA") acknowledges and supports the importance to law enforcement of using lawful interception capabilities to investigate and prevent crime. To that end, TIA and the Alliance for Telecommunications Industry Solutions ("ATIS") have jointly developed the J-STD-025 series of standards to provide law enforcement with the capabilities mandated by the Communications Assistance for Law Enforcement Act of 1994 ("CALEA").

The U.S. Department of Justice has filed a Petition for Expedited Rulemaking ("Petition") challenging the sufficiency of J-STD-025-B as a CALEA standard, as it relates to cdma2000® packet technology. The Petition alleges that the standard omits a number of intercept capabilities required by CALEA and requests that the Commission commence a rulemaking to establish the missing capabilities as legal requirements. The Commission's task at this stage of proceedings is to determine whether to commence the requested rulemaking and the scope of any such rulemaking.

TIA respectfully disagrees that all of the additional capabilities requested by law enforcement are required by CALEA. Rather, a number of them – specifically, the requests for more precise mobile location information and for security, performance and reliability capabilities – have been expressly rejected by the Commission in the past for being beyond the "plain language" of the statute. Accordingly, the Commission should not commence a new rulemaking to again consider those issues that it has spent considerable time and effort deciding in the past.

The Commission should also rule that port number extraction is not required by CALEA. Such information is typically not "call-identifying information" ("CII") that must be extracted under Section 103(a)(2) of CALEA, as the port numbers sought by law enforcement do not

identify the "origin, direction, destination or termination" of a subject's packet data communications. Instead, these port numbers typically describe the higher layer protocol – *i.e.*, the "application" or "content-layer" protocol – with which the data in the packet are associated, and are therefore closely associated with the application or content being accessed by the intercept subject. As a result, such information is properly classified as communications "content" that need only be provided under Section 103(a)(1) of CALEA when a full intercept order is received, if and only if that material is transmitted as part of the data stream associated with the communication.

For all other capabilities requested by law enforcement – such as the provision of Internet Protocol ("IP") addresses and timing information – the Commission would need to issue a notice of proposed rulemaking to determine whether such additional capabilities are encompassed within CALEA's statutory bounds – especially in light of the fact that Congress itself "urge[d] against overbroad interpretation of the requirements" and stated that CALEA should serve as "both a floor and a ceiling" for the requirements."[1] Accordingly, this analysis would involve difficult factual questions, including whether the information is CII and "reasonably available" at the relevant Intercept Access Point ("IAP"); whether the provision of such additional capabilities meets all of the requirements for Commission action under Section 107(b) of CALEA, including the cost-effectiveness requirement;[2] and whether the requested capabilities align with the Commission's technology-neutrality policy and Congressional intent to avoid technology mandates.[3] All of these issues should be carefully considered by the Commission pursuant to a

[1] *See* H.R. Rept. 103-827, at 22 (1994).

[2] *See* H.R. Rept 103-827, at 22 (1994) ("The bill is not intended to guarantee one-stop shopping for law enforcement,").

[3] *See* H.R. Rept. 103-827, at 19 (1994) ("The Committee's intent is that compliance with the requirements in the bill will not impede the development and deployment of new

thorough notice-and-comment proceeding. In order to avoid future litigation, the Commission should resolve these contentious issues only after compiling a fresh and complete factual record that fully comprehends today's technological advances. Moreover, in deciding these issues, the Commission must adhere to the clear legal authority of the CALEA statute itself.

Finally, TIA urges the Commission to seek comment on whether the proposed 12-month period for implementing the additional capabilities requested by law enforcement is reasonable. Based on its experience, a 12-month implementation period is likely to be too short if the Commission were to mandate the capabilities requested by law enforcement, especially if legacy equipment or handsets need to be replaced. Ultimately, though, the reasonableness of a 12-month implementation period will turn on exactly which (if any) of the additional capabilities are found to be required by CALEA.

---

technologies. The bill expressly provides that law enforcement may not dictate system design features and may not bar introduction of new features and technologies."); Senate Rept. 103-402, at 19 (1994) (same).

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
In the Matter of Petition for Expedited	)	
Rulemaking to Establish Technical	)	RM-11376
Requirements and Standards Pursuant to	)	
Section 107(b) of the Communications	)	
Assistance for Law Enforcement Act	)	

To: The Commission

COMMENTS OF THE
TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association ("TIA") hereby comments on the Petition for Expedited Rulemaking ("Petition")[4] filed by the United States Department of Justice ("DOJ" or "law enforcement") challenging the sufficiency of J-STD-025-B as an industry standard for the conduct of lawful intercepts pursuant to Section 107 of the Communications Assistance for Law Enforcement Act of 1994 ("CALEA").[5] Specifically, the Petition alleges that the portions of J-STD-025-B that relate to cdma2000® packet technology[6] fail to provide law enforcement with:

---

[4] *See* Petition for Expedited Rulemaking to Establish Technical Requirements and Standard Pursuant to Section 107(b) of the Communications Assistance for Law Enforcement Act, RM No.11376 (filed May 15, 2007) ("Petition"); Public Notice, Report No. 2816 (rel. May 25, 2007).

[5] Pub. L. 103-414, 108 Stat. 4279 (1994) ("CALEA"), *codified in scattered sections of* Titles 18 and 47 of the United States Code.

[6] The Petition itself is limited to J-STD-025-B as it relates to cdma2000® packet technology. *See* Petition at 1-2 (challenging J-STD-025-B as "the CALEA standard for CDMA2000 packet data wireless services."). DOJ, however, requests that "any rules established by the Commission requiring carriers to provide the additional and/or modified capabilities described herein should also be applicable with respect to other published standards where the same capabilities are at issue." *Id*. at 5 n.10.

(1) the source and destination IP addresses, the transport protocol information in the IP header, and the port numbers for an intercept subject's packet communications;

(2) adequate timing information for such packet communications;

(3) more precise mobile location information that is reasonably available; and

(4) security, performance and reliability capabilities.

TIA acknowledges and supports the importance to law enforcement of having lawful interception capabilities to investigate and prevent and detect crime, including terrorism. To that end, TIA and the Alliance for Telecommunications Industry Solutions ("ATIS") have jointly developed the J-STD-025 series of standards, in consultation with law enforcement, for the conduct of lawfully authorized electronic surveillance.

However, TIA respectfully disagrees with law enforcement that all of the additional capabilities requested by law enforcement in the Petition are required by CALEA. As explained below, the requests for more precise mobile location information and new security, performance and reliability capabilities have been rejected by the Commission in the past for being outside of the scope of CALEA. Port number extraction is also not required by CALEA because port numbers are virtually always associated with the application or content being accessed by the user rather than the "origin, direction, destination or termination" of a communication. For these capabilities, the Commission need not commence a new rulemaking to decide whether they are required by CALEA.

For all of the other capabilities requested by law enforcement, TIA agrees that a thorough notice-and-comment proceeding would be needed to determine whether they are required by the CALEA statute and meet all of the criteria for Commission action in Section 107 of CALEA, thus avoiding the prospect of future litigation. As part of any such proceeding, the Commission should seek comment on the cost-effectiveness of the capabilities being requested by law

enforcement, whether the requested capabilities align with Congressional intent to avoid technology mandates or threaten innovation (*e.g.*, with respect to geo-location solutions), and whether the 12-month implementation period proposed by DOJ is a reasonable and justifiable one. In this endeavor, the Commission must focus on the requirements of the legally-binding statute rather than on what standards groups may have included in other CALEA standards for different technologies as part of the give-and-take of the standards-setting process.

I. THE COMMISSION SHOULD REJECT THE LOCATION, SECURITY, PERFORMANCE AND RELIABILITY CAPABILITIES THAT IT HAS PREVIOUSLY FOUND NOT TO BE REQUIRED BY CALEA

Two of the additional capabilities requested by the Petition – the more precise mobile location information capability and the security, performance and reliability capabilities – have been rejected by the Commission in the past for being outside of the scope of CALEA. The Petition offers no basis for the Commission to revisit those findings today and, accordingly, TIA requests that such capabilities be excluded from any notice of proposed rulemaking issued in response to the Petition.

A. The Commission Has Rejected Previous Requests For More Precise Location Information

In the Petition, DOJ argues that CALEA requires telecommunications carriers to provide all reasonably available signaling information that reveals the location of a mobile handset at the beginning and end of a communication.[7] Specifically, DOJ is seeking more precise location information (such as the altitude, latitude and longitude of the handset) than the cell site location information currently provided under J-STD-025-B.

When J-STD-025-A was challenged in 1999, the Commission considered a similar argument by the New York City Police Department ("NYPD") that "any location information

[7] Petition at 26-40.

that is used and/or is available within a carrier's network for the purpose of providing overall service and/or processing of individual calls"[8] should be provided under CALEA. At that time, the NYPD was similarly "concern[ed] about [the Commission's] proposal to adopt cell site location rather than a more precise location for the subject's mobile terminal."[9] On that occasion, the Commission rejected NYPD's argument on the grounds that "such a capability poses difficulties that could undermine individual privacy" and concluded that "a more generalized capability that will identify only the location of a cell site, and only at the beginning and termination of the call, will give LEAs adequate information."[10]

On appeal, the D.C. Circuit affirmed the Commission's conclusions with respect to location information.[11] In doing so, the court recognized the pivotal role played by privacy in the Commission's decision:

> [T]he Commission's analysis of the location capability did more than just pay lip service to CALEA's privacy requirements. . . . *Expressly relying on CALEA's privacy protection provisions*, . . . the Commission rejected a New York Police Department proposal that would have required triangulating signals from multiple cellular antenna towers to pinpoint a wireless phone's precise location throughout a call's duration.[12]

The Petition acknowledges that the Commission has previously ruled that a more precise mobile location capability is not required under CALEA.[13] It argues, however, that the Commission should revisit this finding because "location identification technology has greatly

---

[8] *Communications Assistance for Law Enforcement Act*, Third Report and Order, 14 FCC Rcd 16794, at ¶ 43 (1999) ("*1999 Third Report and Order*").

[9] *Id*.

[10] *Id*. at ¶ 46.

[11] *See U.S. Telecom Ass'n v. FCC*, 227 F.3d 450, 463-64 (2000) ("*USTA*").

[12] *Id*. at 464 (emphasis added).

[13] Petition at 31-32.

advanced in its ability to precisely locate a wireless handset subscriber" and that carriers now use more precise location technologies to comply with statutory mandates such as E911, for network management, and for some commercial services.[14] But in fact, the unavailability of more precise location information in carriers' networks was never the Commission's reason for rejecting this capability in the first place. Rather, the Commission rested its decision on the more fundamental finding that providing such information would violate the individual privacy protections in CALEA. DOJ offers no reason for thinking that this privacy concern is any less pertinent today than it was in 1999; nor can it offer any justification, as the provision of more precise location information is necessarily a greater invasion of personal privacy than the provision of cell site information.[15]

TIA also notes that the mere fact that some advanced location capabilities have been incorporated into wireless carriers' networks for E911 and other purposes does not mean that such capabilities can be easily invoked for the purposes of lawful interception. When such capabilities were designed, the provision of such precise location information was not contemplated. For many carriers, the network elements that provide location information are separate from the elements used for lawful intercept. Costly network modifications would likely be needed to enable the two systems to operate together seamlessly, with potentially serious impacts on both network performance and on how quickly intercepted information can be

[14] *Id*. at 32-33.

[15] In fact, DOJ has previously defended the inclusion of location capability in J-STD-025-A against challenges by privacy advocates on the grounds that it was limited to cell site information at the beginning and end of a call. *See* Comments Regarding Standards for Assistance Capabilities Requirements at 19-20 ¶ 38 ("[A] wireless carrier can satisfy its obligations under the interim standard by providing cell site information (e.g., 'CELL017') rather than more specific location information. . . . The interim standard is therefore not calculated to allow the 'tracking of' of cellular or PCS subscribers in any specific sense."), *filed in Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213 (filed May 20, 1998).

delivered to law enforcement. For some carriers, advanced location capability has been implemented in the handsets that they sell to subscribers. In such implementations, it may not be possible to activate more precise location capabilities without the subscriber becoming aware of it, which would violate CALEA's transparency requirements. A location capability that is active for all calls would also increase power consumption and drain handset batteries more quickly, which may also be noticed by the intercept subject.

In effect, requiring carriers to provide unobtrusive, advanced location capabilities would force all carriers to implement network-based location capability instead of handset-based capability. This would be inconsistent with the Commission's E911 rules, which allows either kind of location capability to be deployed,[16] and with Congress's intent to avoid technology mandates and protect technological innovation under CALEA by prohibiting law enforcement from dictating system design or constraining technology solutions.[17] Indeed, the Commission should not establish an intercept capability by rule unless it would be consistent with the language and intent of the CALEA statute, and "serve the policy of the United States to encourage the provision of new technologies and services to the public."[18] Imposing a specific technology design or solution – thereby limiting technological innovation by industry – would not be consistent with the statute.

---

[16] *See* 47 C.F.R. §§ 20.18(f) and (g) (establishing phase-in periods for network-based and handset-based location technologies).

[17] *See* H.R. Rept. 103-827, at 19 (1994) ("The Committee's intent is that compliance with the requirements in the bill will not impede the development and deployment of new technologies. The bill expressly provides that law enforcement may not dictate system design features and may not bar introduction of new features and technologies."); Senate Rept. 103-402, at 19 (1994) (same).

[18] CALEA § 107(b)(4), 47 U.S.C. § 1006(b)(4).

For all of these reasons, the Commission should affirm that CALEA does not require carriers to provide any more precise location information than cell site information, and exclude the DOJ's request for such capability from any notice of proposed rulemaking issued in response to the Petition.

B. The Commission Has Held That CALEA Does Not Require Carriers To Implement Any Specific Quality Control Capabilities To Assist Law Enforcement

In the Petition, DOJ also argues that CALEA requires carriers to implement specific security, performance and reliability capabilities to "ensure the protection, completeness, and integrity of communications intercepts."[19] As the Petition explains, "[s]ecurity-related capabilities measure and ensure the overall protection of a given interception," while "[p]erformance- and reliability-related capabilities address the completeness and quality of the information delivered by a telecommunications carrier."[20]

Performance and Reliability Capabilities. With respect to performance and reliability, law enforcement is requesting that carriers be required to ensure that "the quality of the transmission of CII and communications content to law enforcement . . . is at least equal to the highest level of reliability of the carrier's underlying service."[21] DOJ contends that such capabilities are necessary because "CALEA requires that carriers isolate and enable the government to intercept '*all* wire and electronic communications carried by the carrier . . . to or from equipment, facilities, or services of a subscriber' and deliver such intercepted communications to the government."[22]

---

[19] Petition at 40.

[20] *Id*.

[21] *Id*. at 50.

[22] *Id*. at 48.

The Commission, however, has already considered and rejected this argument when it declined to add the surveillance status, continuity check tone and feature status capabilities to J-STD-025-A.[23] In 1999, the DOJ argued that these capabilities were required because Section 103 of CALEA "obligates carriers to take affirmative steps to ensure surveillance integrity."[24] Then, as now, DOJ argued that "a carrier that does not take any affirmative steps to monitor the integrity of authorized electronic surveillance is not 'ensuring' that its equipment facilities, and services are capable of delivering 'all communications' and all reasonably available call-identifying information"[25] to which the government may be entitled under CALEA. The Commission disagreed and ruled instead that: "the plain language of the Act mandates compliance with the assistance capability requirements of section 103(a), *but does not require carriers to implement any specific quality control capabilities to assist law enforcement*."[26] In the same vein, the Commission declared that: "the plain language of the statute mandates compliance with the capability requirements of section 103(a), *but does not require that such capability be proven or verified on a continual basis*."[27] To further emphasize the point, the Commission explained that "[e]nsuring that a wiretap is operational can be done in either a

[23] *1999 Third Report and Order* at ¶¶ 101 (surveillance status), 106 (continuity check tone), 111 (feature status).

[24] *Id*. at ¶ 100. *See also id*. at ¶¶ 105, 110 (same).

[25] *Id*. at ¶ 100.

[26] *Id*. at ¶ 111 (emphasis added).

[27] *Id*. at ¶ 106. *See also id*. at ¶ 101 ("We interpret the plain language of the statute to mandate compliance with the capability requirements of section 103(a), but not to require that such capability be proven or verified on a continual basis.").

technical or non-technical manner, and section 103(a) does not include 'ensurance' itself as a capability."[28] These findings were not challenged on appeal to the D.C. Circuit.[29]

Accordingly, because the "plain language the statute" does not require carriers to provide "any specific quality control capabilities," the performance and reliability capabilities requested in the Petition are also not required by CALEA. The requested capabilities are clearly of the same kind as the "quality control capabilities" previously rejected by the Commission. Indeed, DOJ admits as much by describing the performance and reliability capabilities that it seeks as grounded in "quality of service concerns"[30] and by requesting quantitative measures, such as packet loss and bit error rates, "to assess the quality of the transmission of CII and communications content to law enforcement."[31]

The Petition offers no basis for the Commission to reach a different conclusion today than it did in 1999. DOJ attempts to distinguish the packet-mode services at issue in J-STD-025-B from the circuit-mode services in J-STD-025-A on the grounds that, unlike for circuit-mode services, "the loss of one or more packets may render the collection of an entire communication worthless if the packets lost are vital to the reconstruction of the communication."[32] But even if true, this assertion is irrelevant to the Commission's conclusion that the "plain language" of CALEA does not require carriers to provide such quality control capabilities. This is not to say that law enforcement will have no means of ensuring the reliable delivery of lawfully intercepted packet-mode communications and CII. As the Commission has noted, "[w]e are confident that

[28] *Id*. at ¶ 101. *See also id*. at ¶¶ 106 (same), 111 (same).

[29] *See USTA*, 227 F.3d at 456.

[30] Petition at 43.

[31] *Id*. at 50.

[32] *Id*. at 45.

carriers and LEAs will work together to ensure that a wiretap is functioning correctly, and also note that there is nothing that would prevent carriers from providing this capability either on a voluntary basis, or with compensation from LEAs."[33] Indeed, ATIS is working with law enforcement to prepare a set of technical specifications to assist law enforcement in this regard, outside of the CALEA legal framework.

TIA also notes that the transmission of lawfully intercepted communications and CII to law enforcement is the statutory responsibility of law enforcement. This is reflected in Section 103(a)(3) of CALEA, which provides that carriers need only deliver lawfully intercepted communications and CII "in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier."[34] Clearly, the statute contemplates that the government would procure, *i.e.* pay for, the facilities, equipment and services necessary for the transmission of lawfully intercepted communications and CII to the government.

Law enforcement's attempt to impose performance and reliability capabilities on carriers is therefore not much more than an attempt to impermissibly shift its statutory responsibility away from itself and on to carriers and their customers. This is abundantly clear from law enforcement's suggestion that carriers be required under CALEA to support either collocation of law enforcement's storage equipment or buffering coupled with a later-provisioned Virtual Private Network is a sharp departure from the statutory framework.[35] Tellingly, the Petition's

---

[33] *1999 Third Report and Order* at ¶ 106. *See also id*. at ¶¶ 101, 111 (same).

[34] 47 U.S.C. § 1002(a)(3).

[35] Petition at 49 n.110.

purported reason for creating this obligation is that law enforcement has no desire to provision the high-bandwidth connectivity needed for broadband content intercepts.[36]

Furthermore, the requested performance and reliability capabilities fail to meet the criteria in Section 107(b) for Commission action, as such capabilities would discourage carriers from offering innovative high-bandwidth services to the public and would not represent the most cost-effective solution. Specifically, each time a carrier considers whether to deploy a high-bandwidth service, it would have to consider the buffering requirements that could be available throughout its network at any intercept access point. Alternatively, it would have to give away valuable collocation space to law enforcement. Whether by imposing network investment burdens or by occupying valuable collocation space, the solutions identified by law enforcement will impede the deployment of innovative high-bandwidth services to the public. TIA is concerned that this would occur at precisely the time when video applications are set to become a much more significant part of broadband communications. For these reasons as well, the Commission should not initiate a rulemaking on this previously rejected portion of law enforcement's request.

Security capabilities. The security capabilities requested by law enforcement are more difficult to characterize, mainly because they are described in very general terms.[37] At least one of the security capabilities, however, is clearly a kind of "quality control" capability that the Commission has previously rejected as being beyond the scope of CALEA. Specifically, the capability to "securely deliver" intercepted data to law enforcement[38] is as much a quality control

[36] *Id*. ("Mandating that law enforcement agencies procure a dedicated, high-bandwidth facility from the carrier to law enforcement would be neither a cost-effective nor a time-efficient solution to the problem.").

[37] *See* Petition at 46-47.

[38] *Id*. at 46.

mechanism as the capability to ensure the reliable transmission of such data and both are closely related to the performance of the transmission link between the carrier and law enforcement. As the Commission has consistently held, such capabilities are beyond the "plain language" of CALEA. Accordingly, the Commission should reject law enforcement's request for this particular capability as well. Again, this does not mean that transmissions to law enforcement will not be secure. As with other quality control mechanisms, law enforcement is free to procure secure transmission from the carrier or make other arrangements for secure delivery.

The other security capabilities requested by law enforcement simply state outcomes – *e.g.*, "the capability to ensure that LAES [lawfully authorized electronic surveillance] is unobtrusive"[39] or "the capability to protect the assistance capabilities used to facilitate LAES"[40] – without specifying how those outcomes are to be achieved within the carrier's networks. Many of these security capabilities simply reflect specific obligations in CALEA itself – *e.g.*, "the capability to prevent unauthorized communications and CII from being intercepted."[41] If law enforcement's intent is to simply incorporate such general statements into J-STD-025-B, then it is difficult to see the value in granting the request. Various parts of J-STD-025-B make reference to these general obligations, [42] and all carriers understand that they have obligations

[39] *Id*.

[40] *Id*.

[41] *Id*. *Compare with* CALEA § 103(a)(4) (requiring carriers to have the capability to "facilitate[e] authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects–(A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and (B) information regarding the government's interception of communications and access to call-identifying information.").

[42] *See*, *e.g.*, J-STD-025-B at §§ 5.3.1.1, 5.3.1.2, 5.3.2.1, 5.3.2.4, 5.3.2.5.

under CALEA to isolate the intercept subject's communications and to ensure that lawful intercepts are unobtrusive.

If, however, law enforcement's request for security capabilities is merely the opening salvo in an attempt to dictate how carriers should design their networks to facilitate "secure" intercepts, then TIA would remind the Commission that the Congressional intent of CALEA was to avoid technology mandates or threaten innovation (*e.g.*, with respect to geo-location solutions). Moreover, CALEA clearly prohibits law enforcement from "requir[ing] any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services."[43] This provision was intended by Congress to prevent technology mandates and thus avoid impeding technological innovation.[44] As noted above, the Commission may not establish an additional capability by rule under Section 107 of CALEA unless it would "serve the policy of the United States to encourage the provision of new technologies and services to the public."[45] Imposing a specific technology design or solution – thereby limiting technological innovation by industry – would not be consistent with this requirement.

Given the lack of clarity in the Petition with respect to the security capabilities, the Commission should decline to consider law enforcement's request for such capabilities until such time as the meaning of those capabilities has been clarified and explained. Such action is

[43] CALEA § 103(b)(1), 47 U.S.C. § 1002(b)(1).

[44] *See* H.R. Rept. 103-827, at 19 (1994) ("The Committee's intent is that compliance with the requirements in the bill will not impede the development and deployment of new technologies. The bill expressly provides that law enforcement may not dictate system design features and many not bar introduction of new features and technologies."); Senate Rept. 103-402, at 19 (1994) (same).

[45] CALEA § 107(b)(4), 47 U.S.C. § 1006(b)(4).

warranted because, as it now stands, the record is simply insufficient for the Commission to initiate a rulemaking or to frame meaningful questions. Moreover, industry cannot properly respond to law enforcement's security proposals without a better understanding of what they mean.

II. PORT NUMBERS ARE TYPICALLY NOT CALL-IDENTIFYING INFORMATION

The Commission should also not entertain any further, law enforcement's request for port numbers to be provided as CII. Virtually all port numbers are not "call-identifying information" that must be extracted under Section 103(a)(2) of CALEA. "Call-identifying information" is defined by Section 102(2) of CALEA to mean:

> dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier.[46]

The Commission has interpreted "origin," "direction," "destination" and "termination" by reference to "a party or place" from or to which a call is initiated, received or redirected.[47] The port numbers sought by law enforcement, however, do not identify a "party" or a "place" from or to which a communication is made, received or redirected, nor are they used by a telecommunications carrier's network to route a subject's packet data communications. In an IP (Internet Protocol) network,[48] only the IP addresses contained in the IP header of a packet are used for routing purposes. In contrast, port numbers reside in the TCP (Transfer Control

[46] 47 U.S.C. § 1001(2).

[47] *See Communications Assistance for Law Enforcement Act*, Order on Remand, 17 FCC Rcd 6896, at ¶ 47 (2002) ("*Order on Remand*").

[48] TIA notes that a wireless carrier that deploys cdma2000® may not always be the Internet service provider ("ISP") operating the IP-based network. Where an over-the-top ISP is involved, law enforcement would have to serve a relevant court order on that ISP to obtain the IP-related information it wants.

Protocol) or UDP (User Datagram Protocol) header of a packet. They are used by the devices at the communication end points to identify the higher level application with which the data in the packet is associated. Certain port numbers are associated with certain Internet applications. For example, ports 20 and 21 are associated with the File Transfer Protocol used for transferring files, port 25 is associated with the Simple Mail Transfer Protocol, while port 80 is associated with the HyperText Transfer Protocol used for transferring web pages.[49]

In other words, while IP addresses tell the routers where to send packets, port numbers typically tell the computers at the communication end points what kind of data is in the packet, *i.e.*, they describe the application or content layer protocol associated with the contents of the packet so that the end-point computers know how to process the packet. In this regard, port numbers are like the "[o]ther dialing tones that may be generated by the sender that are used to signal customer premises equipment of the recipient," which Congress has explained "are not to be treated as call-identifying information."[50] As a result, port numbers are properly classified as communications content that need only be provided upon a showing of probable cause and when a full Title III intercept order is received,[51] and not CII that must be provided on receipt of a pen register or trap-and-trace order.[52] While CALEA does not use the term "contents" or define what it means, the term is defined in federal wiretap statutes to "include[] any information concerning

[49] *See* http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers (last visited May 18, 2007).

[50] H.R. Rept. 103-827, at 21 (1994). *See also* Senate Rept. 103-402, at 21 (1994) (same).

[51] *See* 18 U.S.C. § 2518.

[52] *See* 18 U.S.C. §§ 3123, 3124.

the substance, purport, or meaning of that communication."[53] Port numbers clearly meet this definition, as they describe the kind of information contained inside the packet.

The Petition attempts to confuse the issue by describing the port numbers it seeks as the numbers "used to identify the ends of logical connections that carry conversations, which typically consist of multiple packets exchanged between endpoints,"[54] and as "endpoint[s] for network communications."[55] This is true if one understands the ends of a logical connection as being an application like a web browser or an email program, rather than distinct parties or physical locations. As between two computers communicating with each other over the Internet, many "logical connections" can be established for different applications, each with different port numbers. However, the fact remains that the actual, physical end points of those communications are still the two computers, as identified by their IP addresses and not by their port numbers. The port numbers only help the computers segregate – by application type – the different streams of communications in which their users may be engaged.

For all of these reasons, the Commission should reject law enforcement's request for port number extraction under CALEA.

III. A THOROUGH NOTICE-AND-COMMENT PROCEEDING WOULD BE NEEDED TO DETERMINE WHETHER OTHER CAPABILITIES ARE REQUIRED BY CALEA

For other capabilities requested by law enforcement (such as the provision of IP addresses and timing information), TIA submits that a thorough notice-and-comment proceeding would be required to determine whether they are required by CALEA and whether they meet all of the criteria for Commission action in Section 107 of CALEA. The same searching scrutiny

[53] 18 U.S.C. § 2510(8).

[54] Petition at 14.

[55] Petition at 15.

should also be applied to any capability discussed in Part I or II, *supra*, that the Commission decides it should reconsider.

A. The Requested Capabilities Must Meet the Requirements of Section 107(b)

Under Section 107(b) of CALEA, the Commission may only establish, by rule, assistance capability requirements alleged to be missing from a industry standard if those requirements meet certain criteria. Specifically, the Commission may only establish requirements or standards that:

> (1) meet the assistance capability requirements of section 103 by cost-effective methods;
>
> (2) protect the privacy and security of communications not authorized to be intercepted;
>
> (3) minimize the cost of such compliance on residential ratepayers;
>
> (4) serve the policy of the United States to encourage the provision of new technologies and services to the public; and
>
> (5) provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under section 103 during any transition period.

Thus, not only must the capabilities in question meet the requirements of Section 103 of CALEA, they must also meet the cost-effectiveness, privacy, security and other requirements of Section 107 before the Commission may adopt it as a legal requirement. While the Petition attempts to address each of these criteria, it is clear that the Commission should seek more input from interested parties. The requirements of Section 103 and Section 107 of CALEA can raise difficult legal, policy and factual issues, such as:

- whether the information sought by law enforcement is CII;
- whether the CII in question is "reasonably available" to the carrier (or to someone else) at the relevant Intercept Access Point;

- whether a carrier will be "unduly burdened" with network modifications if required to implement a CII capability;
- whether an intercept capability is "cost effective," especially in view of the Commission's decision that carriers cannot recover their costs of CALEA implementation as part of their intercept provisioning costs;[56]
- whether a capability will enable lawfully authorized interceptions to take place unobtrusively;
- the impact of a capability on the privacy and security of communications and CII not authorized to be intercepted;
- whether a capability protects information regarding the government's interception of communications and access to call-identifying information;
- the effect of requiring a capability on the prices for residential services;
- whether an intercept capability will dictate particular network or service designs, thereby comprising a technology mandate; and
- the impact of requiring a particular capability on technological innovation and service deployment.

In considering these questions, the Commission should be guided by the requirements of the statute and not by what other standards groups may have agreed to include in other CALEA standards as part of the give-and-take of the standards-setting process. Industry standards for CALEA are established through a negotiated process conducted by various standards bodies in consultation with law enforcement. It is not surprising, therefore, that the standards-setting process may yield different results for different network technologies, and include compromises, such as the inclusion of non-CALEA capabilities. Thus, when one standards body decides to

[56] *See Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Second Report and Order and Memorandum Opinion and Order, 21 FCC Rcd 5360, at ¶¶ 70-71 (2006) ("*2006 Second Report and Order*") (concluding that CALEA § 109, 47 U.S.C. § 1008, is the "exclusive" mechanism for carriers to recover their CALEA implementation costs). *Compare Order on Remand* at ¶ 60 (concluding that the "punch list" items were cost effective in part because "carriers can recover at least a portion of their CALEA software and hardware costs by charging to LEAs, for each electronic surveillance order authorized by CALEA, a fee that includes recovery of capital costs, as well as recovery of the specific costs associated with each order.").

include a particular capability in its CALEA standard while another does not, neither body can be accorded much deference regarding whether the capability in question is required by CALEA as a matter of law. Moreover, just because one standards body decides to include a non-CALEA capability in a standard for one kind of technology does not mean that that capability should be extended blindly to all other technologies without an independent evaluation of the statute's requirements. As the Commission has said:

> [M]anufacturers and carriers are free to develop and deploy additional features and capabilities beyond those required by CALEA in efforts to assist law enforcement agencies in conducting lawfully-authorized electronic surveillance. Such capabilities, however, will not be subject to any of CALEA's obligations, including cost recovery, *and will not affect any party's obligations under CALEA in any way*.[57]

B. The Commission Must Revisit Its Cost Effectiveness Criteria to Take Into Account Obsolete Cost Recovery Rules

In deciding whether a particular capability should be required by CALEA, a key question that the Commission must consider is whether the capability meets the requirements of Section 103 "by cost-effective methods." Indeed, failure to properly consider "cost effectiveness" was one of the main reasons for the D.C. Circuit's decision to remand the four challenged "punch list" items in the Commission's *1999 Third and Report Order* for further consideration.[58]

On remand in 2002, the Commission conducted additional cost analysis and concluded that the four "punch list" items were "cost-effective." The Commission based this conclusion, in part, on its findings that the "DoJ/FBI will be paying for many of the costs associated with implementing the four vacated punch list capabilities," and that "carriers can recover at least a portion of their CALEA software and hardware costs by charging to LEAs, for each electronic

---

[57] *See Communications Assistance for Law Enforcement Act*, Further Notice of Proposed Rulemaking, 13 FCC Rcd 22632, at ¶ 35 (1998) (emphasis added).

[58] *USTA*, 227 F.3d at 461-62.

surveillance order authorized by CALEA, a fee that includes recovery of capital costs, as well as recovery of the specific costs associated with each order."[59]

This is no longer true. In its *2006 Second Report and Order*, the Commission concluded that "carriers bear responsibility for CALEA development and implementation costs for post-January 1, 1995 equipment and facilities."[60] Thus, in stark contrast to the Commission's findings in 2002, the federal government will no longer be "paying for many of the costs associated with implementing [CALEA]" for post-1995 equipment, except on the very rare occasion in which a carrier is able to prove that compliance with a particular capability is not "reasonably achievable" under the stringent 11-factor test in Section 109(b) of CALEA.[61] The Commission went on to hold that Section 109(b) was the "*exclusive*" method of cost recovery under CALEA, and therefore reversed its previous finding that carriers could recover at least a part of their CALEA implementation costs through intercept provisioning charges:

> [Carriers] are prohibited by CALEA from recovering through intercept charges the costs of making modifications to equipment, facilities, or services pursuant to the assistance capability requirements of CALEA section 103 and the costs of developing, installing, and deploying CALEA-based intercept solutions that comply with the assistance capability requirements of CALEA section 103.[62]

Because all of the equipment and facilities that are potentially affected by DOJ's latest Petition will be post-1995 equipment, they will be subject to these new rules which prohibit cost recovery. It follows that the Commission must evaluate the cost-effectiveness of the additional capabilities requested in the Petition in light of these new rules. It cannot simply discount the

---

[59] *Order on Remand* at ¶ 60.

[60] *2006 Second Report and Order* at ¶ 70.

[61] *Id*. *See* 47 U.S.C. § 1008(b).

[62] *2006 Second Report and Order* at ¶ 71.

financial burden that the requested capabilities will place on carriers on the ground that the costs will be borne by the government.

C. The Commission Should Not Impede Technological Innovation by Imposing Any Specific Technology or Technological Solution

When Congress enacted CALEA, it took steps to ensure that "the requirements in [CALEA] will not impede the development and deployment of new technologies."[63] It did so by denying law enforcement the authority to "to require any specific design of equipment, facilities, services, features or system configurations to be adopted," or "to prohibit the adoption of any equipment, facility, service or feature," by any provider of wire or electronic communications services.[64] It also directed the Commission not to impose any requirements under CALEA unless it would "serve the policy of the United States to encourage the provision of new technologies and services to the public."[65] Imposing a specific technology design or solution (*e.g.*, with respect to geo-location) – thereby limiting technological innovation by industry – would not be consistent with this requirement or Congressional intent.

The Commission must respect that Congressional directive any time additional capabilities are requested by law enforcement. Elsewhere in these Comments, TIA has already identified a number of ways in which some of the capabilities requested by law enforcement could discourage the provision of new services and features to consumers. The Commission needs to conduct this same kind of analysis for all of the additional capabilities requested by law enforcement.

---

[63] H.R. Rept. 103-827, at 19; Senate Rept. 103-402, at 19.

[64] CALEA § 103(b)(1); 47 U.S.C. § 1002(b)(1).

[65] CALEA § 107(b)(4); 47 U.S.C. § 1006(b)(4).

Moreover, while the Petition appears to be limited to J-STD-025-B and cdma2000® packet technologies, it potentially has a much greater reach. Law enforcement has explicitly requested that "any rules established by the Commission requiring carriers to provide the additional and/or modified capabilities described herein should also be applicable with respect to other published standards where the same capabilities are at issue."[66] While it is questionable whether CALEA allows the Commission to revise standards that have not been formally challenged under Section 107, the Commission's decision in this proceeding could have precedential value beyond J-STD-025-B and cdma2000®, and therefore its potential impact on other technologies cannot be ignored.

D. The Commission Must Provide Reasonable and Justifiable Time and Conditions for Compliance With Any New Capabilities That It Establishes

To the extent that the Commission does decide to add capabilities to J-STD-025-B, the Commission must also "provide a reasonable time and conditions for compliance" with the new requirements.[67] In this regard, law enforcement has proposed a 12-month implementation period. Based on its experience, TIA does not believe that this would be a reasonable period for carriers to implement the additional capabilities requested in the Petition. As law enforcement is aware and the Commission has seen, software enhancement cycles are 18 months or more, while the replacement cycle for network and handset hardware advances will be even longer. Of course, the time it will take to implement any new capabilities may depend on the specific capabilities that the Commission decides to establish by rule. Accordingly, the Commission should seek comment on what would constitute a reasonable implementation period for any new capabilities.

---

[66] Petition at 5 n.10.

[67] CALEA § 107(b)(5), 47 U.S.C. § 1006(b)(5).

IV. CONCLUSION

For the reasons set forth above, the Commission should dismiss those parts of the Petition that request capabilities that have been previously rejected or which are plainly not required by CALEA, and commence a notice-and-comment proceeding to thoroughly consider all other parts of the Petition.

Respectfully submitted,

/s/

Grant Seiffert, President
Danielle Jafari, Senior Director
and General Counsel, Government Affairs
Telecommunications Industry Association
2500 Wilson Blvd., Suite 300
Arlington, VA 22201
Tel: 703-907-7700
Fax: 703-907-7727

Of Counsel:

Thomas M. Barba
Chung Hsiang Mah
Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036
Tel: 202-429-3000
Fax: 202-429-3902

July 20, 2007